UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/858,085	05/15/2001	Ali Sheikh	13095:11	2540

7590 11/18/2004

William N. Hulsey III
HULSEY GRETHER & FORTKORT LLP
8911 N Capital of Texas Hwy
Suite 3200
Austin, TX 78759

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 11/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/858,085	SHEIKH ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/1/02; 3/5/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 have been examined.

Priority

2. Receipt is acknowledged of papers filed under 35 U.S.C. 119 (e) based on an application filed in United States Provisional application on 11/29/00. Applicant has not complied with the requirements of 37 CFR 1.63(c), since the oath, declaration or application data sheet does not acknowledge the filing of any United States Provisional application. A new oath, declaration or application data sheet is required in the body of which the present application should be identified by application number and filing date.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko et al. United States Letters Patent Number 6,789,202 in view of Rothermel et al. United States Letters Patent Number 6,678,827.

As per claim 1:

Ko et al. teach a method of monitoring a plurality of security parameters for a networked system having a first server and at least one second server, the networked system having a transport communication layer, the transport communication layer having a master transport located on the first server, the method comprising the steps of:

comparing a data set located within a resident program located on the at least one second server (Col. 6, lines 30-31; within local analyzers these policies are compiled into specifiers for local sensors; Col. 6, lines 36-37; the system then allows local sensors to implement the specified sensors; **computer with local analyzer reads on second server**) against a rule set generated by a user; (Col. 6, lines 23-25; global policy can be received from a network security coordinator)

generating a result forwardable to the master transport based on the step of comparing; (Col. 7; lines 14-15; sensors are then configured to report attacks to critical servers to local analyzers)

collecting the results in the first server; and (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer; **computer with global analyzer reads on first server**)

Ko et al. do not explicitly disclose a method comprising reporting the results from the first server to the user.

Rothermel et al. in analogous art, however, teach a method comprising reporting the results from the first server to the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the network security information can be reported to users such as system administrators so that they can verify that the security policy is correctly implemented.

As per claim 2:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method wherein the first server concurrently performs other networking tasks during the steps of comparing, generating, collecting, or reporting. (Col. 6; lines 39-41; during normal operations of networked computer

system, local analyzers receive security information from local sensors) (Col. 6; lines 52-53; global analyzer uses this information to determine a global response to the global security condition)

As per claim 3:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method wherein the step of comparing is performed by an agent transport located on the at least one second server. (Col. 6, lines 42-43; local analyzers examine security information; **local analyzer reads on agent transport**)

As per claim 4:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method wherein at least one second server concurrently performs other networking tasks during the steps of comparing, generating, collecting, or reporting. (Col. 6; lines 39-44; during normal operations of networked computer system, local analyzers receive security information from local sensors)

As per claim 5:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method comprising: providing a list of one or more sensor programs for comparing data sets in a task list resident in the agent transport. (Col. 5; lines 48-49; a sensor can be constructed from a host-based intrusion detection system, a network sniffer, a firewall)

As per claim 6:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method comprising: accessing, by the agent transport, the task list; (Col. 6, lines 31-31; within local analyzers, global policies are compiled into specifiers for local sensors) and selecting a resident program to monitor. (Col. 6; lines 36-37; the system then allows local sensors to implement the specified sensors)

As per claim 7:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method comprising selectively accessing, by the transport agent, a sensor program on the second server. (Col. 4; lines 5-6; local analyzers communicate with sensors located within the computer systems)

As per claim 8:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method wherein the step of comparing performed at least in part by the sensor program. (Col. 5, lines 41-43; sensor can be configured dynamically by analyzer to detect a specific security-related events and local intrusions)

As per claim 9:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method comprising: reordering the task list. (Col. 5; lines 44-45; sensor can additionally be tuned to quickly react to on-going large-scale intrusions in a manner that is consistent with a global policy)

As per claim 10:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method wherein the sensor program is responsible for monitoring an as yet unmonitored program resident on the second server. (Col. 5; lines 41-45; sensor can be configured dynamically by analyzer to detect a specific security-related events and local intrusions within the assigned portion of networked computer system.)

As per claim 11:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method wherein the comparing by two or more sensor programs generates reportable results. (Col. 5, lines 47-48; different sensors can include different intrusion detection response capabilities)

As per claim 12:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further teach a method the step of reordering comprising adding a sensor program. (Col. 5, lines 48-50; a sensor can be constructed from a host-based intrusion detection system, a network sniffer, a firewall or a wrapper.)

As per claim 13:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Rothermel et al. further teach a method wherein the reportable results are combined into a single transportable packet. (Col. 1, lines 38-40; network information is often transmitted as a series of individual packets of information)

As per claim 14:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Rothermel et al. further teach a method wherein the agent transport encrypts the forwardable result. (Figure 9, item 933; Col. 5, lines 56-58; any of the information transmitted between the network security devices and the supervisor devices and the manager device can be protected from unauthorized access by encrypting information)

As per claim 15:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Rothermel et al. further teach a method wherein the master transport decrypts the forwardable result. (Figure 10, item 1017; Col. 5, lines 56-58; any of the information transmitted between the network security devices and the supervisor devices and the manager device can be protected from unauthorized access by encrypting information)

As per claim 16:

Ko et al. teach a method for monitoring a security parameter for a network, the network having a first and a second server, the first server having a transport mechanism communicatively connected to the second server, the method comprising the steps of:

monitoring at one or more times for changes to a firewall policy; (Col. 6, lines 23-25; global policy can be received from a network security coordinator;) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting on the first server the changes to the firewall policy; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

the second server performing other networking tasks concurrently with the steps of collecting, storing, compiling, or reporting. (Col. 6; lines 39-44; during normal operations of networked computer system, local analyzers receive security information from local sensors)

Ko et al. further disclose a sensor can be constructed from a host-based intrusion detection system (IDS), a network sniffer a firewall or a wrapper that intercepts the arguments of system calls. This makes it possible to reuse existing intrusion detection capabilities on networked computer system in order to implement a system that enforces global intrusion detection policies. (Col. 5, lines 48-52). Sensor for a firewall policy detection can be implemented on the same structure discussed above in claim 1.

Ko et al. do not explicitly disclose a method comprising storing the changes to the firewall policy on the first server; compiling a history of the changes to the firewall policy on the first server; and reporting the history of the firewall policy changes; and

Rothermel et al. in analogous art, however, teach a method comprising

storing the changes to the firewall policy on the first server; (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling a history of the changes to the firewall policy on the first server; (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information; **manager device reads on first server**)

reporting the results from the first server to the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the firewall policy change can be reported to users such as system administrators so that they can verify that the firewall policy is correctly implemented.

As per claim 17:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Rothermel et al. further disclose a method comprising the steps of: monitoring whether a change is an approved change; archiving changes into a first report, the report identifying approved changes. (Col. 5, lines 32-39; as the network security device executes and implements its specific security policy, the network security device gathers network security information about its activities and about the network information that is monitored and forwards it to supervisor devices)

As per claim 18:

Ko et al. further disclose a method comprising the steps of:

monitoring information on an administrator of a networking policy change; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on the administrator of the networking policy changes; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving one or more sets of information on the administrator; and compiling the one or more sets of information on the administrator of the networking policy changes, the user able to view the compiled information in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving one or more sets of information on the administrator; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more sets of information on the administrator of the networking policy changes, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to

include a method comprising archiving one or more sets of information on the administrator; and compiling the one or more sets of information on the administrator of the networking policy changes, the user able to view the compiled information in a format determinable by the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the information on the administrator of a network policy change can be reported to users such as system administrators so that they can verify that the administrator of a network policy change is correctly implemented.

As per claim 19:

Ko et al. and Rothermel et al. further disclose a method further comprising the steps of:

monitoring the time of the administrator's networking policy changes; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting the time of the administrator's networking policy changes; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving one or more sets of times of the administrator's networking policy changes; and compiling the one or more sets of time of the administrator's networking policy changes, the user able to view the compiled time in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving one or more sets of times of the administrator's networking policy changes; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more sets of time of the administrator's networking policy changes, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled time in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Rothermel et al. further disclose the network information can also include information about the logging itself, such as a time stamp, the action taken after applying filter rules, and information about the supervisor/host device such as the device name, corresponding process name, and corresponding process ID. (Col. 12, lines 5-9)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create

consistent security policy for multiple network security devices and follow-up its implementation. This way, the information on the administrator of a network policy change can be reported to users such as system administrators so that they can verify that the administrator of a network policy change is correctly implemented.

As per claim 20:

Ko et al. and Rothermel et al. further disclose a method comprising the steps of:

collecting the firewall policy change that is pushed (Col. 6, lines 23-25; global policy can be received from a network security coordinator) to the firewall policy; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving one or more sets of firewall policy information that is pushed to the firewall policy; and compiling the one or more sets of firewall policy information that is pushed to the firewall policy, the user able to view the compiled firewall policy information that is pushed in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving one or more sets of firewall policy information that is pushed to the firewall policy; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more sets of firewall policy information that is pushed to the firewall policy, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled firewall policy information that is pushed in a format

determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the firewall policy change can be reported to users such as system administrators so that they can verify that the firewall policy is correctly implemented.

As per claim 21:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. and Rothermel et al. further disclose a method further comprising the step of:

establishing one or more baselines by an administrator for a system on the network; (Col. 6, lines 23-25; global policy can be received from a network security coordinator)

monitoring the one or more baselines established by an administrator; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the one or more baselines into a baseline report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving a one or more baseline reports of the changes; and compiling the one or more baseline reports, the user able to view the compiled information in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving a one or more baseline reports of the changes; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more baseline reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been

obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy by establishing a baseline for multiple network security devices and follow-up its implementation. This way, the network security information can be monitored and reported to users such as system administrators so that they can verify establishing one or more baseline and its implementation.

5. Claims 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko et al. United States Letters Patent Number 6,789,202 in view of Rothermel et al. United States Letters Patent Number 6,678,827 and further in view of Teng United States Letters Patent Number 5,812,763.

As per claim 22:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the step of:

monitoring one or more operating system's file integrity on the network; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the one or more operating system's file integrity into a file integrity report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more file integrity reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more file integrity reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

Neither of the references, however, explicitly disclose a method about a file integrity on the network.

Teng in analogous art, however, discloses a system file protection inspector that performs a series of probe operations in connection with protection of each file system to find those which have improper protection levels. (Col. 4; lines 39-43)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. and Rothermel et al. to include a method about a file integrity on the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Teng (Col. 2, lines 49-50) in order to protect each file by including a protection code. This way, the level of protection is not only at the network level but also includes the files that are stored in each computer that is connected to the network system.

As per claim 23:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the step of:

monitoring a Web server's configuration file; (Col. 6, lines 23-25; global policy can be received from a network security coordinator;) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the Web server's configuration file into a Web Server's configuration report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more Web Server's configuration reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more Web Server's configuration reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

As per claim 24:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the step of:

monitoring a proxy server's configuration file; (Col. 6, lines 23-25; global policy can be received from a network security coordinator; **computer with global analyzer reads on proxy server**) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the proxy server's configuration file into a proxy server's configuration file report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more proxy server's configuration file reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more proxy server's configuration file reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

As per claim 25:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose comprising the step of:

monitoring a user's password strength; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on the password's strength into a password strength report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more password strength report; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more password strength report, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators).

The rationale for combining the above references is the same basis as claim 16 above.

Neither of the references, however, explicitly disclose a method about a file integrity on the network.

Teng in analogous art, however, discloses a password inspector that detects whether a user who is authorized to use the computer system has selected a password, which can be easily guessed (Col. 4; lines 1-3)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. and Rothermel et al. to include a method about user's password strength on the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Teng (Col. 4, lines 14-16) in order to protect the network system from unauthorized users. This way, the password strength is checked to avoid easy guessing by another person who is not authorized to use the system.

6. Claims 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko et al. United States Letters Patent Number 6,789,202 in view of Rothermel et al. United States Letters Patent Number 6,678,827 and in view of Teng United States Letters Patent Number 5,812,763 and further in view of Cromer et al. 6,263,441.

As per claim 26:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the step of:

establishing a one or more events that triggers an alert; (Col. 6, lines 23-25; global policy can be received from a network security coordinator)

monitoring for the one or more alert triggering events; (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

providing an alert notice upon the occurrence of the one or more alert triggering event. (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Not explicitly disclosed by Ko et al. and Rothermel et al. is that events that triggers an alert.

Cromer et al. in analogous art, however, disclose detecting a change to a configuration of the computer system, using detection logic of the computer, and generating an alert associated with any change in the configuration in real time.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. and Rothermel et al. to include a method about events that triggers an alert on the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Cromer et al. (Col. 2, lines 29-31) in order to provide a method of notifying a remote server when key system components are removed or added or changed to a networked computer.

As per claim 27:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the steps of:

collecting information on the one or more alert triggering event into a alert report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose

archiving the one or more alerts reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more alert reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

As per claim 28:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Rothermel et al. further disclose a method comprising the step of: monitoring encrypted secure connections between the first and the one or more second servers. (Col. 5, lines 56-58; any of the information transmitted between the Network security device and the supervisor devices and the manager device can be protected from unauthorized access by encrypting information)

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Coss et al. U.S. No. 6,154,775

This reference pertains to an improved computer network firewalls which include one or more features for increased processing efficiency.

b. Antur et al. U.S. No. 6,243,815

This reference pertains to a method of reconfiguring network security devices coupled to a network directory services server.

c. Trcka et al. U.S. No. 6,453,345

This reference pertains to a network security and surveillance system passively monitors and records the traffic present on a local area network or wide area network.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
Examiner
Art Unit 2133

11/10/04